Retrieving Reed-Solomon coded data under interpolation-based list decoding

Jianwen Zhang, *Student Member, IEEE*

Marc A. Armand, *Member, IEEE*

Abstract

A transform that enables generator-matrix-based Reed-Solomon (RS) coded data to be recovered under interpolation-based list decoding is presented. The transform matrix needs to be computed only once and the transformation of an element from the output list to the desired RS coded data block incurs k^2 field multiplications, given a code of dimension k.

Index Terms

Galois Field Fourier Transform, list decoding, Reed-Solomon codes

I. INTRODUCTION

Since their inception in 1958, Reed-Solomon (RS) codes have found widespread use, e.g., in compact discs (CDs), digital video broadcasting and high definition TV. Let Φ be a cyclic subgroup of $\mathrm{GF}(q)\backslash\{0\}$ of order n and α its generator. Then, following its original definition, $\{(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n : c_i = m(\alpha^i),\ 0 \leq i \leq n-1,\ m(x) = \sum_{j=0}^{k-1} m_j x^j \in \mathrm{GF}(q)[x]\}$ is an (n, k) RS code over $\mathrm{GF}(q)$ with zeros $\alpha, \alpha^2, \ldots, \alpha^{n-k}$. In practice however, data is typically not encoded via the evaluation map

$$\begin{aligned} E_\Phi &: \mathrm{GF}(q)^k \mapsto \mathrm{GF}(q)^n \\ &: (m_0, m_1, \ldots, m_{k-1}) \rightarrow (m(1), m(\alpha), \ldots, m(\alpha^{n-1})) \end{aligned} \tag{1}$$

Jianwen Zhang, and Marc A. Armand are with the Department of Electrical & Computer Engineering, National University of Singapore, 119260. (Email:{jianwen.zhang, elema}@nus.edu.sg)

implied by this definition. On the other hand, the interpolation-based RS list decoders of [1], [2] which allow far more errors to be corrected than previously thought possible, operate on the assumption that messages are encoded via an evaluation map. Incorporating such a decoder within an existing system employing RS codes is clearly desirable. For instance, it will allow a system to operate at a significantly lower signal-to-noise ratio while maintaining the same error performance. Nevertheless, incorporating such a decoder into an existing system requires the ability to recover the original RS coded data from the output list of this decoder. For the CD player for example, this would mean that we will not have to replace all our existing CDs. A method for recovering generator-matrix-based RS coded data under interpolation-based list decoding is therefore desirable as well.

Such a method has implicitly been introduced in the proof of [3, Lemma 4]. The main idea there is as follows. Let $v_0, v_1, \ldots, v_{n-1}$ be nonzero elements of GF(q). Then the codeword $(c_0, c_1, \ldots, c_{n-1})$ of an (n, k) generalized RS code defined by a basis of codewords given by the rows of the matrix

$$\mathcal{G} = \begin{pmatrix} v_0 & v_1 & \ldots & v_{n-1} \\ v_0 & v_1\alpha & \ldots & v_{n-1}\alpha^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_0 & v_1\alpha^{k-1} & \ldots & v_{n-1}\alpha^{(k-1)(n-1)} \end{pmatrix} \tag{2}$$

and the codeword $(c_0/v_0, c_1/v_1, \ldots, c_{n-1}/v_{n-1})$ of an (n, k) RS code defined by a different basis of codewords given by the rows of the matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \alpha & \ldots & \alpha^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \ldots & \alpha^{(k-1)(n-1)} \end{pmatrix}$$

correspond to the same message. Thus, suppose the message $(m_0, m_1, \ldots, m_{k-1})$ is encoded via multiplication by $\mathcal{G}$ and the resulting codeword transmitted and received as $(r_0, r_1, \ldots, r_{n-1})$. Provided less than $n - \sqrt{(k-1)n}$ errors occur during transmission, the decoder of [1], operating on the premise that messages are encoded via the evaluation map in (1), generates a list containing $(m_0, m_1, \ldots, m_{k-1})$ when applied to the modified received

word $(r_0/v_0, r_1/v_1, \ldots, r_{n-1}/v_{n-1})$. The underlying basis transformation thus results in an overhead of n multiplications to the overall decoding complexity. The above method is however no longer applicable when the generator matrix $\mathcal{G}$ is not of the form in (2), e.g. when $\mathcal{G}$ has the same structure as the matrix in (5).

This correspondence presents a more general solution to the aforementioned problem in that our technique remains applicable given *any* generator matrix $\mathbf{G}_a$ for an RS code. Since $\mathbf{G}_a$ is arbitrary, the underlying basis transformation employed in our approach is different to that used in [3] - see Lemma 1 below. In fact, if messages are encoded as codewords of a narrow-sense RS code, *no* basis transformation is needed. For code rates of practical interest, an average computational overhead of $O(k^2)$ multiplications is added to the decoding process.

We exploit certain properties of the Galois Field Fourier Transform (GFFT), including the fact that encoding a message block $(m_0, m_1, \ldots, m_{k-1})$ via the evaluation map in (1) is equivalent to computing the GFFT of the n-tuple $(m_0, m_1, \ldots, m_{k-1}, 0, \ldots, 0)$ – a consequence of property 2 of [4, Theorem 8-13]. Our main result is Theorem 1 in Section III below. However, before we can prove this theorem, we need a few lemmas. For the remainder of this correspondence, take the evaluation map to mean that specified by (1). Further, take an interpolation-based list decoder to mean an instance of the decoders of [1], [2].

II. LEMMAS LEADING TO THE KEY RESULT

Without loss of generality, let q be a fixed power of 2. Suppose $\mathcal{C}$ is an (n, k) RS code over GF(q) with generator polynomial $g(x) = \prod_{i=b}^{n-k-1+b}(x - \alpha^i) = \sum_{i=0}^{n-k} g_i x^i$. We do not assume that $b = 1$ so that $\mathcal{C}$ is not necessarily a narrow-sense RS code.

Lemma 1. *Let*

$$\mathbf{W} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha^{(b-1)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha^{(b-1)(n-1)} \end{pmatrix}.$$

If $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$*, then* $\bar{\mathbf{c}} = \mathbf{c} \times \mathbf{W}$ *is a codeword of a narrow-sense* (n, k) *RS code* $\bar{\mathcal{C}}$ *over* GF(q).

Proof: Let the code polynomial for $\mathbf{c}$ and $\bar{\mathbf{c}}$ be written as $c(x) = \sum_{i=0}^{n-1} c_i x^i$ and $\bar{c}(y)$. Then

$$c(x) = \sum_{i=0}^{n-1} c_i \alpha^{(b-1)i} \left(\frac{x}{\alpha^{b-1}}\right)^i = \sum_{i=0}^{n-1} \bar{c}_i y^i = \bar{c}(y), \tag{3}$$

where $\bar{c}_i = c_i \alpha^{(b-1)i}$, $y = \frac{x}{\alpha^{b-1}}$. Since $c(x)$ has zeros $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{n-k-1+b}$, $\bar{c}(y)$ clearly has zeros $\alpha, \alpha^2, \ldots, \alpha^{n-k}$ and the lemma follows. ■

Next, let $\bar{g}(y) = \sum_{i=0}^{n-k} \bar{g}_i y^i$ where $\bar{g}_i = g_i \alpha^{(b-1)i}$. Since $\bar{g}(y)$ may not be monic, it is a code polynomial, but not necessarily, the generator polynomial of $\bar{\mathcal{C}}$. The following matrix is nevertheless

$$\bar{\mathbf{G}} = \begin{pmatrix} \bar{g}_0 & \bar{g}_1 & \cdots & \bar{g}_{n-k} & 0 & \cdots & 0 \\ 0 & \bar{g}_0 & \cdots & \bar{g}_{n-k-1} & \bar{g}_{n-k} & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \bar{g}_{n-k} \end{pmatrix}. \tag{4}$$

a valid generator matrix for $\bar{\mathcal{C}}$, since the rows of $\bar{\mathbf{G}}$ spam a vector space over GF(q) of dimension k. Let $[\mathbf{U}]$ denote the $n \times n$ matrix resulting from appending $n-k$ rows to a $k \times n$ matrix ($n > k$) $\mathbf{U}$ such that each additional row is a right cyclic shift of the previous row by one position. Lemma 2 shows the relation between $[\bar{\mathbf{G}}]$ and $[\mathbf{G}]$ where

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & g_{n-k} \end{pmatrix} \tag{5}$$

is a generator matrix for the code $\mathcal{C}$.

Lemma 2. $[\mathbf{G}] \times \mathbf{W} = \mathbf{W} \times [\bar{\mathbf{G}}]$.

Proof: Denote the first row of $[\mathbf{G}]$ and $[\bar{\mathbf{G}}]$ by $(g_0, g_1, \ldots, g_{n-1})$ and $(\bar{g}_0, \bar{g}_1, \ldots, \bar{g}_{n-1})$, respectively. Thus, $g_j = \bar{g}_j = 0$ for $n-k+1 \leq j \leq n-1$. Since α has order n by definition, the element of $[\mathbf{G}]$ and $[\bar{\mathbf{G}}]$ located at the $(s+1)^{th}$ row and $(t+1)^{th}$ column, where $0 \leq s, t \leq n-1$, are $g_{t-s \bmod n}$ and $\bar{g}_{t-s \bmod n} = g_{t-s \bmod n} \alpha^{(b-1)t} / \alpha^{(b-1)s}$, respectively.

Hence, $[\bar{\mathbf{G}}]$ may be obtained by multiplying the $(t+1)^{th}$ column of $[\mathbf{G}]$ by $\alpha^{(b-1)t}$ and dividing the $(s+1)^{th}$ row of the resultant matrix by $\alpha^{(b-1)s}$. In matrix form, $[\bar{\mathbf{G}}] = \mathbf{W}^{-1} \times [\mathbf{G}] \times \mathbf{W}$. ■

Let $\mathbf{F}$ and $\mathbf{F}^{-1}$ denote the n-point GFFT and inverse GFFT matrices over GF(q), ie.

$$\mathbf{F} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \cdots & \alpha^{(n-1)(n-1)} \end{pmatrix}, \tag{6}$$

$$\mathbf{F}^{-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(n-1)} & \cdots & \alpha^{-(n-1)(n-1)} \end{pmatrix}. \tag{7}$$

Lemma 3 gives a decomposition of $[\bar{\mathbf{G}}]$ in terms of $\mathbf{F}$ and $\mathbf{F}^{-1}$.

Lemma 3. $[\bar{\mathbf{G}}] = \mathbf{F}^{-1} \times \mathbf{D} \times \mathbf{F}$ *where* $\mathbf{D}$ *is an* $n \times n$ *diagonal matrix such that its main diagonal is the inverse GFFT of the first row of* $[\bar{\mathbf{G}}]$.

Proof: Let the inverse GFFT of the first row of $[\bar{\mathbf{G}}]$ be $\mathbf{G}(1) = (G_0, G_1, \ldots, G_{n-1})$. Since the $(i+1)^{th}$ row of $[\bar{\mathbf{G}}]$ is the right cyclic shift of the first row of $[\bar{\mathbf{G}}]$ by i positions, it follows from the modulation property of GFFT [5, Figure 6.1] that the inverse GFFT of the $(i+1)^{th}$ row of $[\bar{\mathbf{G}}]$ is

$$\mathbf{G}(i+1) = (G_0, G_1/\alpha^i, G_2/\alpha^{2i}, \ldots, G_{n-1}/\alpha^{(n-1)i}).$$

Consequently, the inverse GFFT of the rows of $[\bar{\mathbf{G}}]$ in matrix form may be expressed as

$$[\bar{\mathbf{G}}] \times \mathbf{F}^{-1} = \begin{pmatrix} G_0 & G_1 & G_2 & \cdots & G_{n-1} \\ G_0 & G_1/\alpha & G_2/\alpha^2 & \cdots & G_{n-1}/\alpha^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ G_0 & G_1/\alpha^{n-1} & G_2/\alpha^{2(n-1)} & \cdots & G_{n-1}/\alpha^{(n-1)(n-1)} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(n-1)} & \alpha^{-2(n-1)} & \cdots & \alpha^{-(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} G_0 & 0 & \cdots & 0 \\ 0 & G_1 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & G_{n-1} \end{pmatrix}$$

$$= \mathbf{F}^{-1} \times \begin{pmatrix} G_0 & 0 & \cdots & 0 \\ 0 & G_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_{n-1} \end{pmatrix} = \mathbf{F}^{-1} \times \mathbf{D} \tag{8}$$

The lemma is now immediate. ■

Since $\bar{g}(x)$ has zeros $\alpha, \alpha^2, \ldots, \alpha^{n-k}$, it follows from property 2 of [4, Theorem 8-13] that the last $n-k$ elements of $\mathbf{G}(1)$ and in turn, the last $n-k$ elements in the main diagonal of $\mathbf{D}$, are all zero. Moreover, since $\bar{g}_i = g_i \alpha^{(b-1)i}$, by the translation property of the GFFT [5, Figure 6.1], the inverse GFFT $(G_0, G_1, \ldots, G_{k-1}, 0, \ldots, 0)$ of the n-tuple $(\bar{g}_0, \bar{g}_1, \ldots, \bar{g}_{n-k}, 0, \ldots, 0)$ is the right cyclic shift of the inverse GFFT of the n-tuple $(g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0)$ by $b-1$ positions.

III. THE KEY RESULT

In this section, we present a method for retrieving from the output list of an interpolation based list decoder, messages encoded as codewords of the RS code $\mathcal{C}$ via a generator matrix $\mathbf{G}_a$ given by $\mathbf{G}_a = \mathbf{A} \times \mathbf{G}$ for some $k \times k$ basis transformation matrix $\mathbf{A}$. We assume that the decoder operates on the premise that messages are encoded as codewords of $\bar{\mathcal{C}}$ via the evaluation map.

Let $\tilde{\mathbf{A}} = (\ \mathbf{A} \quad \mathbf{0}\ )$ be a $k \times n$ matrix where $\mathbf{0}$ is a $k \times (n-k)$ all-zero matrix. In addition, let $\mathbf{U}_{i \times j}$ denote the $i \times j$ upper-left submatrix of $\mathbf{U}$. Further, since the evaluation map may be interpreted as the n-point GFFT over GF(q), the relation between a codeword $\bar{\mathbf{c}}$ of $\bar{\mathcal{C}}$ and its preimage $(f_0, f_1, \ldots, f_{k-1}) \in GF(q)^k$ under this map may be expressed as $\bar{\mathbf{c}} = \mathbf{f} \times \mathbf{F}$ where $\mathbf{f} = (f_0, f_1, \ldots, f_{k-1}, 0, \ldots, 0)$. We can now prove our main result, ie., Theorem 1.

Theorem 1. *Let* $\mathbf{m} \in$ GF$(q)^k$ *be encoded as* $\mathbf{c} \in \mathcal{C}$ *via the generator matrix* $\mathbf{G}_a$*. Then* $\mathbf{m}^T = (\mathbf{A}^T)^{-1} \times (\mathbf{W}_{k \times k})^{-1} \times (\mathbf{F}^{-1}_{k \times k})^{-1} \times (\mathbf{D}_{k \times k})^{-1} \times (\mathbf{f}_{1 \times k})^T$.

Proof: By Lemmas 1 to 3,

$$\begin{aligned}\bar{\mathbf{c}} &= \mathbf{c}\times\mathbf{W} = \mathbf{m}\times\mathbf{G}_a\times\mathbf{W} = \mathbf{m}\times\mathbf{A}\times\mathbf{G}\times\mathbf{W}\\ &= \mathbf{m}\times\tilde{\mathbf{A}}\times[\mathbf{G}]\times\mathbf{W} = \mathbf{m}\times\tilde{\mathbf{A}}\times\mathbf{W}\times[\bar{\mathbf{G}}]\\ &= \mathbf{m}\times\tilde{\mathbf{A}}\times\mathbf{W}\times\mathbf{F}^{-1}\times\mathbf{D}\times\mathbf{F}. \qquad (9)\end{aligned}$$

Since $\bar{\mathbf{c}} = \mathbf{f}\times\mathbf{F}$, we have $\mathbf{f} = \mathbf{m}\times\tilde{\mathbf{A}}\times\mathbf{W}\times\mathbf{F}^{-1}\times\mathbf{D}$. Moreover, since $\mathbf{F}$, $\mathbf{F}^{-1}$, $\mathbf{D}$ and $\mathbf{W}$ are symmetric,

$$\mathbf{f}^T = \mathbf{D}\times\mathbf{F}^{-1}\times\mathbf{W}\times\tilde{\mathbf{A}}^T\times\mathbf{m}^T. \qquad (10)$$

Since the last $n-k$ elements in the main diagonal of $\mathbf{D}$ as well as in the column vector $\tilde{\mathbf{A}}^T\times\mathbf{m}^T$ are all zero, the last $n-k$ constraints in (10) vanish and so (10) may be reduced to $(\mathbf{f}^T)_{k\times 1} = \mathbf{D}_{k\times k}\times(\mathbf{F}^{-1}\times\mathbf{W})_{k\times k}\times(\tilde{\mathbf{A}}^T\times\mathbf{m}^T)_{k\times 1}$. Because $\mathbf{W}$ is diagonal, $(\mathbf{F}^{-1}\times\mathbf{W})_{k\times k} = \mathbf{F}^{-1}_{k\times k}\times\mathbf{W}_{k\times k}$. Moreover, $(\tilde{\mathbf{A}}^T\times\mathbf{m}^T)_{k\times 1} = \mathbf{A}^T\times\mathbf{m}^T$ and since $\mathbf{F}^{-1}_{k\times k}$, $\mathbf{D}_{k\times k}$, $\mathbf{W}_{k\times k}$ and $\mathbf{A}$ are all invertible, it follows that $\mathbf{m}^T = (\mathbf{A}^T)^{-1}\times(\mathbf{W}_{k\times k})^{-1}\times(\mathbf{F}^{-1}_{k\times k})^{-1}\times(\mathbf{D}_{k\times k})^{-1}\times(\mathbf{f}_{1\times k})^T$. ■

Interpreting $\mathbf{f}_{1\times k}$ and $\mathbf{m}$ in Theorem 1 as an element of the output list and the desired data block, respectively, leads to Algorithm 2 below which summarizes the key steps involved to recover any generator-matrix-based RS coded data from the output list of an interpolation-based list decoder.

Algorithm 2.

Input: The zeros $(\alpha^b, \alpha^{b+1}, \ldots, \alpha^{n-k-1+b})$ *of* $\mathcal{C}$ *and its generator matrix* $\mathbf{G}_a$.

Output: The desired messages corresponding to the elements of the output list.

Precomputation (to be performed only once):

i. *Compute* $g(x) = \prod_{i=0}^{n-k-1}(x-\alpha^{b+i}) = \sum_{i=0}^{n-k} g_i x^i$ *and construct the matrix* $\mathbf{G}$ *for which the* $(i+1)^{th}$ *row,* $0 \le i \le n-1$, *is the right cyclic shift of the* n*-tuple* $(g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0)$ *by* i *positions.*

ii. *Find* $\mathbf{A}$ *such that* $\mathbf{G}_a = \mathbf{A}\times\mathbf{G}$ *and* $(\mathbf{A}^T)^{-1}$. *(Note: The matrix* $\mathbf{A}$ *can be easily found using standard techniques in linear algebra since* $\mathbf{G}$ *is in row echelon form.)*

iii. *Compute the inverse GFFT of the* n*-tuple* $(g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0)$. *Then right cyclic shift the resultant vector by* $b-1$ *positions to obtain* $(G_0, G_1, \ldots, G_{k-1}, 0, \ldots, 0)$.

iv. *Set* $(D_{k\times k})^{-1} = diag(G_0^{-1}, G_1^{-1}, \ldots, G_{k-1}^{-1})$ *and* $(\mathbf{W}_{k\times k})^{-1} = diag(1, \alpha^{-(b-1)}, \alpha^{-2(b-1)}, \ldots, \alpha^{-(k-1)(b-1)})$.

v. *Compute* $(\mathbf{F}_{k\times k}^{-1})^{-1}$ *and* $\mathbf{B} = (\mathbf{A}^T)^{-1} \times (\mathbf{W}_{k\times k})^{-1} \times (\mathbf{F}_{k\times k}^{-1})^{-1} \times (D_{k\times k})^{-1}$. *(Note: Since* $\mathbf{F}_{k\times k}^{-1}$ *is symmetric, its inverse can be computed by eigenvalue decomposition.)*

List decoding & message recovery:

1. *Compute* $\bar{\mathbf{r}} = \mathbf{r} \times \mathbf{W} = (r_0, r_1\alpha^{(b-1)}, \ldots, r_{n-1}\alpha^{(n-1)(b-1)})$ *where* $\mathbf{r}$ *is the hard-decision received vector.*
2. *List decode* $\bar{\mathbf{r}}$.
3. *If the output list is not empty, then for each element* $\mathbf{f}_{1\times k}$ *in this list, return* $\mathbf{B} \times (\mathbf{f}^T)_{k\times 1}$.

A few remarks are in order. First, since the average list size is typically very close to unity [6] [2], Steps 1) & 3) will incur close to k^2+n-1 GF(q)-multiplications on average. Thus, for code rates of practical interest, an average computational overhead of $O(k^2)$ multiplications is introduced on top of the computations incurred by Step 2). Second, if $b = 1$, $\mathbf{W}$ reduces to an identity matrix such that $\mathbf{W}_{k\times k}$ may be omitted in the computation of $\mathbf{B}$. Finally, if messages were originally encoded by multiplication by $g(x)$, then $\mathbf{G}_a = \mathbf{G}$ in this case with $\mathbf{A}$ reducing to an identity matrix.

Example 1. *Let* $\mathcal{C}$ *be a* $(7, 4)$ *RS code over* GF(8) *with zeros* $\alpha^2, \alpha^3, \alpha^4$. *Its generator matrix is*

$$\mathbf{G}_a = \begin{pmatrix} \alpha^5 & \alpha & \alpha^3 & \alpha & \alpha^3 & \alpha^2 & \alpha \\ \alpha^6 & 0 & \alpha^4 & \alpha^3 & \alpha^6 & 1 & \alpha^2 \\ \alpha^6 & \alpha^2 & \alpha^2 & \alpha^2 & 0 & \alpha^5 & \alpha^6 \\ \alpha^4 & \alpha^6 & \alpha^3 & \alpha^2 & 1 & 0 & \alpha \end{pmatrix}.$$

Following Algorithm 2, we obtain

$$(\mathbf{A}^T)^{-1} = \begin{pmatrix} \alpha^2 & 1 & \alpha^2 & 0 \\ \alpha^2 & \alpha & \alpha^2 & \alpha \\ \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 \\ \alpha^6 & \alpha^3 & \alpha^2 & \alpha \end{pmatrix}.$$

Applying the inverse GFFT to $(g_0, g_1, g_2, g_3, 0, 0, 0) = (\alpha^2, \alpha^3, 1, 1, 0, 0, 0)$ *and right cyclic shifting the resulting vector by* 1 *position yields* $(G_0, G_1, G_2, G_3, 0, 0, 0) = (\alpha^6, \alpha^5, 1, \alpha^5, 0, 0, 0)$ *and so* $(\mathbf{D}_{4\times4})^{-1} = diag(\alpha, \alpha^2, 1, \alpha^2)$. *Now,* $(\mathbf{W}_{4\times4})^{-1} = diag(1, \alpha^6, \alpha^5, \alpha^4)$ *and*

$$(\mathbf{F}_{4\times4}^{-1})^{-1} = \begin{pmatrix} \alpha^4 & \alpha^3 & \alpha^5 & \alpha^3 \\ \alpha^3 & 1 & 0 & \alpha \\ \alpha^5 & 0 & \alpha^3 & \alpha^2 \\ \alpha^3 & \alpha & \alpha^2 & \alpha^6 \end{pmatrix}.$$

Hence,

$$\mathbf{B} = (\mathbf{A}^T)^{-1} \times (\mathbf{W}_{k\times k})^{-1} \times (\mathbf{F}_{k\times k}^{-1})^{-1} \times (D_{k\times k})^{-1} = \begin{pmatrix} \alpha^5 & \alpha^3 & \alpha & \alpha \\ \alpha^4 & \alpha^5 & \alpha^3 & 1 \\ \alpha^5 & \alpha^2 & 1 & \alpha \\ \alpha & \alpha & \alpha^2 & \alpha \end{pmatrix}. \tag{11}$$

Suppose the codeword $\mathbf{c} = (\alpha^2, 0, \alpha, 0, 0, \alpha^3, \alpha^6)$ *is transmitted and received as* $\mathbf{r}$. *If list decoding the vector* $\bar{\mathbf{r}} = \mathbf{r} \times \mathbf{W}$ *is successful,* $\mathbf{f} = (\alpha, 0, \alpha^5, 1, 0, 0, 0)$ *will be in the output list. We can recover the original message* $\mathbf{m}^T = \mathbf{B} \times \mathbf{f}_{4\times1}^T = (\alpha^3, \alpha^2, 0, \alpha^5)^T$. *It can be verified that* $\mathbf{c} = \mathbf{m} \times \mathbf{G}_a$.

IV. CONCLUSION

To summarize, we have established a relationship between codewords resulting from generator-matrix-based encoding, and codewords obtained via the evaluation map. We have further derived from this relationship, an algorithm for recovering generator-matrix-based coded data under interpolation-based list decoding.

References

[1] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1757–1767, 1999.

[2] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 46, pp. 2809–2825, 2003.

[3] V. Guruswami and A. Vardy, "Maximum-likelihood decoding of Reed-Solomon codes is NP-hard," *IEEE Trans. Inf. Theory*, vol. 51, pp. 2249–2256, July 2005.

[4] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Prentice Hall, 1995.

[5] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge University Press, 2003.

[6] R. J. McEliece, "On the average list size for the Guruswami-Sudan decoder," *7th. International Symposium on Communication Theory and Applications*, pp. 2–6, 2003.